OFFICE OF THE SPECIAL INSPECTOR GENERAL FOR IRAQ RECONSTRUCTION

Review of Data Entry and General Controls in the Collecting and Reporting of the Iraq Relief and Reconstruction Fund

SIGIR-06-003
April 28, 2006

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE **28 APR 2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE
Review of Data Entry and General Controls in the Collecting and Reporting of the Iraq Relief and Reconstruction Fund

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Office of the Special Inspector General for Iraq Reconstruction,400 Army Navy Drive,Arlington,VA,22202-4704

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR’S ACRONYM(S)

11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**32**	

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18

SPECIAL INSPECTOR GENERAL FOR IRAQ RECONSTRUCTION

April 28, 2006

MEMORANDUM FOR U.S. AMBASSADOR TO IRAQ
DIRECTOR, IRAQ RECONSTRUCTION MANAGEMENT OFFICE
COMMANDING GENERAL, GULF REGION DIVISION, U.S. ARMY CORPS OF ENGINEERS

SUBJECT: Audit Report on Review of Data Entry and General Controls in the Collecting and Reporting of the Iraq Relief and Reconstruction Fund (SIGIR-06-003)

We are providing this audit report for your information and use. We performed the audit in accordance with our statutory duties contained in Public Law 108-106, as amended, which requires that we provide for the independent and objective conduct of audits, as well as leadership and coordination of and recommendations on policies designed to promote economy, efficiency, and effectiveness in the administration of Iraq relief and reconstruction programs and operations and to prevent and detect waste, fraud, and abuse.

We considered management comments from the U.S. Ambassador to Iraq, the Iraq Reconstruction Management Office, and the Gulf Region Division, U.S. Army Corps of Engineers, on a draft of this report when preparing the final report.

We appreciate the courtesies extended to the staff. For additional information on this report, please contact in Baghdad, Iraq, Mr. Joseph T. McDermott at (703) 343-7926, or by email at joseph.mcdermott@iraq.centcom.mil; or Mr. Clifton Spruill at (703) 343-9275, or by email at clifton.spruill@iraq.centcom.mil. For the report distribution, see Appendix D.

Stuart W. Bowen, Jr.
Inspector General

cc: Distribution

Special Inspector General for Iraq Reconstruction

SIGIR-06-003 **April 28, 2006**

Review of Data Entry and General Controls in the Collecting and Reporting of the Iraq Relief and Reconstruction Fund

Executive Summary

Introduction. In November 2005, we initiated this audit to determine whether policies, procedures, and internal controls established by U.S. government organizations ensure valid and reliable data for management of over 13,000 Iraq Relief and Reconstruction Fund (IRRF) projects with a total value of $18.4 billion.

To improve overall management of IRRF projects and funds and to improve the reporting to Congress and the other senior U.S. decision makers, the development of an information technology (IT) management reporting system was initiated by the Project and Contracting Office (PCO) in mid-2004. By mid-2005 the IT system was only partially operational and was not being utilized by all of the agencies receiving IRRF funds. In September 2005, the U.S. Army Corps of Engineers, Gulf Region Division (GRD) and PCO officials briefed the Iraq Reconstruction Management Office (IRMO) Director on a recommended solution requiring consolidation of information from multiple data sources into a single database. The proposed integrated U.S. government IT solution was named the Iraq Reconstruction Management System (IRMS). GRD-PCO[1] is responsible for maintaining the operational and security aspects of IRMS.

Ensuring the security and integrity of the data in the computer systems that support critical operations and decision making has never been more important because of concerns about attacks from individuals and groups with malicious intent, including terrorists. These concerns are well founded for a number of reasons, including the dramatic increase in reported computer security incidents, the ease of obtaining and using hacking tools, and the steady advance in the sophistication and effectiveness of attack technology.

Further, internal control procedures specific to data entry provide the initial level of confidence that helps ensure completeness, accuracy, and validity of all transactions during processing. It is the basis for establishing the integrity of the data contained in the IRMS.

This audit report is one of a series of reports addressing the IT and management information systems being used to support the IRRF programs and their ability to produce reliable and accurate information.

Objective. The objective of this audit was to determine whether policies, procedures, and internal controls established by U.S. government organizations ensure valid and reliable data for effective management of Iraq reconstruction projects. Specifically, this report addresses internal control procedures used to assure integrity of data entering the IRMS and the general controls relating to the IRMS system itself. The review did not address controls over individual applications within IRMS.

[1] Effective December 4, 2005, the PCO was merged with the U.S. Army Corps of Engineers, Gulf Region Division, to form GRD-PCO.

Results. The development of policies and procedures to validate the data being entered into IRMS has been ad hoc at best. Management officials of the GRD-PCO Communications and Information Technology function[2] (GRD-PCO G-6) stated that they rely on the organizations owning the data to provide the quality assurance controls on the security and accuracy of the data being provided to IRMS. However, our discussions with officials at the U.S. Agency for International Development and Multi-National Security Transition Command-Iraq, who are owners of data; as well as our review of other audit reports, identified a lack of documented internal control procedures to validate the data being entered into systems that subsequently provide input to IRMS.

In assessing general controls over IRMS, we used the U.S. Government Accountability Office, "Federal Information System Controls Audit Manual". We reviewed GRD-PCO practices that were either under construction or implemented. Several of the supporting documents plus processes that were not documented appear to be a good start in developing a quality security management program. Some of control elements that were partially implemented, included access controls, data back-up, and data retention. We also identified specific vulnerabilities and the lack of official policies and procedures within GRD-PCO G-6 in the following general control areas:

- security program planning and management
- access controls
- application software development and change controls
- system software
- segregation of duties
- service continuity

Conclusion. The reliability of the reports generated by IRMS is diminished without assurance that the initial data entering the system are complete, accurate, and valid. Internal control procedures specific to data entry are critical in providing the initial level of confidence that helps ensure completeness, accuracy, and validity of all transactions during processing. It is the basis for establishing the integrity of the data contained in the IT system. In addition, well-designed and properly implemented IT general controls are essential to protect GRD-PCO's computer resources and operational environment from the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations.

For IRMS general controls, GRD-PCO has taken many important steps to implement an information security program. However, key elements of such a program have not been fully implemented. Weaknesses in information security controls have placed IRMS financial and management information at risk. Implementing an effective information security program could help ensure that known weaknesses affecting the IRMS computing resources are promptly mitigated and that general controls effectively protect its computing environment. Until such improvements are made, there is diminished assurance that there is adequate security and integrity of the data in IRMS that supports program management oversight and decision making.

[2] Army organizations have an alpha/numeric designator which identifies their various command functions, for example, G-2 = Intelligence, G-4 = Logistics, etc. The Communications and Information Technology function is identified by G-6.

It is important for IRMO, in coordination with the GRD-PCO and the agencies utilizing IRRF, to continue to provide active leadership in assuring all organizations work together in correcting the problems identified with IRMS.

Recommendations. We recommend that the Director of the Iraq Reconstruction Management Office develop and issue a policy requiring all organizations entering data into IRMS to have documented internal control procedures that require validation of all data entering the system.

We also recommend that the Commanding General GRD-PCO direct the GRD-PCO G-6 Director of Information Technology to:

- Review all operating procedures of the security management program to ascertain if they contain current and accurate information and are still applicable to the operation. Those operating procedures which are still valid should then be formally signed and dated by GRD-PCO G-6 Director of IT. Once formalized, the procedures should be distributed and discussed with the IT staff responsible for implementing the procedure, referenced to the IT Security Plan (if applicable), and kept on-site at various locations for reference.

- Document and formalize a security plan for IRMS. The basis for a GRD-PCO IT security plan is contained in the GRD-PCO G-6 draft document, "System Security Authorization Agreement" (SSAA), dated September 6, 2005. A review of the draft SSAA should be conducted to update existing information and to ensure that it contains all required elements, as prescribed by OMB Circular A-130, including such topics as application rules and contingency planning. The updated security plan should then be approved by GRD-PCO G-6 Director of IT. Multiple copies of the security plan should be available with some stored at off-site locations.

- Ensure that the access control policy posted on the network server room door is adhered to. All unauthorized personnel should be escorted whenever access to the network server room is required, and not left unattended while in the room. In addition, for control purposes, GRD-PCO G-6 should establish a visitor log to document all personnel escorted into the network server room.

- Develop adequate application software development policies and procedures to establish a formal configuration control process for IRMS. At a minimum, this policy should address the authority of the Configuration Control Board, the requirements authorization and approval process, and the configuration management tracking processes. Policies and procedures should also clearly identify the duties and responsibilities of those identified in the design, development, review, and approval of the system modifications.

- Develop adequate application software development testing policies and procedures to clearly define, at a minimum: the testing methodology to be used; the development of specifications and requirements to be tested; required documentation to be recorded and retained; and levels of testing and associated procedural differences with each level.

- Develop adequate system software control policies and procedures to clearly define, at a minimum: procedures for identifying, selecting, installing, and modifying system software; required documentation to be recorded and retained; and levels of testing and associated procedural differences with each level.

- Develop policies and procedures to clearly delineate separation of duties and responsibilities, including those performed by application programmers, system programmers, and data center, security, and quality assurance staff.

- Develop a contingency plan for restoring critical applications, which includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations. Multiple copies of the contingency plan should be available, with additional copies stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable. In addition, the plan should be tested on an on-going basis to determine whether it will function as intended in an emergency situation. A copy of the contingency plan should be kept in the installation's Security Plan.

Management Comments and Audit Response. A combined response to the draft of this report was received from the U.S. Ambassador of Iraq and IRMO. The U.S. Ambassador to Iraq concurred with the recommendation to develop and issue a policy requiring all organizations entering data into IRMS to have documented internal control procedures that require validation of all data entering the system. The Information Management Unit of IMRO will take the lead. The comments received are fully responsive.

Comments to the draft of this report were also provided by the Commanding General, Gulf Region Division, and have been incorporated into this final report as appropriate. The Commanding General, Gulf Region Division, concurred with all findings in the report and has initiated corrective action on all recommendations. The comments received are fully responsive.

Table of Contents

Introduction

Background

This audit report is one of a series of reports addressing the information technology (IT) and management information systems being used to support the Iraq Relief and Reconstruction Fund (IRRF) programs and their ability to produce reliable and accurate information. In October 2005, we initiated this audit to focus on the policies, procedures, and controls established for data entry and the general controls associated with the Iraq Reconstruction Management System (IRMS). We reported on the evolution of IRMS in a separate report[3].

On November 6, 2003, Congress passed the "Emergency Supplemental Appropriations Act for Defense and for the Reconstruction of Iraq and Afghanistan" Public Law 108-106. The Iraq Relief and Reconstruction Funds (IRRF) section of the legislation consists of a total of $18.4 billion which is allocated by the U.S. government for the rebuilding of Iraq. Section 2207 of the Act required the Director of the Office of Management and Budget (OMB), no later than January 5, 2004, and prior to the initial obligation of funds appropriated under the IRRF, to report on the proposed uses of the funds on a project-by-project basis and to continue to report quarterly on the uses of these funds.

Iraq Reconstruction Management Office (IRMO). National Security Presidential Directive 36, "United States Government Operations in Iraq," May 11, 2004, delegated responsibility for the continuous supervision and general direction of all assistance for Iraq to the Secretary of State. The Directive also created a temporary organization within the U.S. Mission in Iraq, called the Iraq Reconstruction Management Office (IRMO), to facilitate the transition in Iraq.

Project and Contracting Office (PCO). National Security Presidential Directive 36 also established the Project and Contracting Office (PCO) and directed the PCO to provide acquisition and project management support for activities in Iraq. On June 22, 2004, the Deputy Secretary of Defense established the PCO within the Department of the Army and directed the PCO to provide support for all activities associated with financial, program, and project management for both construction and non-construction IRRF activities. The PCO was consolidated with the U.S. Army Corps of Engineers, Gulf Region Division (GRD); to form GRD-PCO on December 4, 2005.

Section 2207 Report. Section 2207 of Public Law 108-106 requires a report from the Office of Management and Budget to the Congress every three months that updates the proposed uses of all IRRF funds on a project by project basis, including estimates of the cost required to complete each project. The Section 2207 Report is compiled by IRMO from data provided by the Department of State, the Department of Defense, the U.S. Agency for International Development (USAID), and other agencies that use IRRF.

Iraq Reconstruction Management System (IRMS). To monitor IRRF projects and funds, the development of an IT management reporting system was initiated by the PCO in mid-2004. PCO's IT management system was called the PCO Solution. The PCO Solution was planned to be a collection of integrated commercial and government applications that would provide management oversight and reporting capabilities on IRRF projects.

[3] *Management of Iraq Relief and Reconstruction Fund Program: The Evolution of the Iraq Reconstruction Management System*, SIGIR-06-001, April 2006.

By mid-2005 the PCO Solution was only partially operational and was not being utilized by all of the agencies receiving IRRF funds. In September 2005, GRD and PCO officials briefed the IRMO Director on a recommended solution to consolidate information from multiple data sources into a single database[4]. The current integrated U.S. government IT solution is named the Iraq Reconstruction Management System (IRMS). GRD-PCO is responsible for maintaining the operational and security aspects of IRMS.

Objective

The objective of this audit was to determine whether policies, procedures, and internal controls established by U.S. government organizations ensure valid and reliable data for effective management of Iraq reconstruction projects. Specifically, this report addresses internal control procedures used to assure integrity of data entering the IRMS and the general controls relating to the IRMS system itself. The review did not address controls over individual applications within IRMS.

For a discussion of the audit scope, methodology, and a summary of prior coverage, see Appendix A. For definitions of the acronyms used in this report, see Appendix C. For a list of the audit team members, see Appendix E.

[4] Briefing presentation entitled, *Consolidated Reconstruction Database Update to Ambassador Speckhard,”* September 5, 2005.

Data Entry Internal Control Procedures

Internal control procedures specific to data entry provide the initial level of confidence that helps ensure completeness, accuracy, and validity of all transactions during processing. These procedures are the basis for establishing the integrity of the data contained in the IT system. Controls include both the routines contained within the computer program code as well as the policies and procedures associated with user activities, such as manual measures performed by the user to determine that the data were processed accurately by the computer[5]. Some of the various control techniques used for data entry ensure completeness and accuracy include the following:

- all authorized transactions are entered into and processed by the computer
- reconciliations are performed to verify data completeness and accuracy
- data entry design features contribute to data accuracy
- data validation and editing are performed to identify erroneous data
- erroneous data are captured, reported, investigated and promptly corrected
- output reports are reviewed to help maintain data accuracy and validity

Management officials of the GRD-PCO Communications and Information Technology function[6] (GRD-PCO G-6) stated that they rely on the organizations owning the data to provide the quality assurance controls on the security and accuracy of the data being provided to IRMS. Our discussions with officials at the U.S. Agency for International Development and the Department of Defense Multi-National Security Transition Command-Iraq, who are owners of IRRF data; as well as our review of other audit reports, identified a lack of documented internal control procedures to validate the data being entered into systems that subsequently provide input to IRMS. In many instances where IRRF organizations have developed procedures to validate the data being entered, they are ad hoc at best.

Some organizations stated that they use automated edits built into the unique application software. In some instances, particularly financial management operations, automated edits work in conjunction with manual edits. However, this does not preclude the need for documented internal controls which require some type of quality assurance review and acceptance of all data as it enters the applications that provide data to IRMS. Documented operating procedures are particularly important in this operating environment where personnel rotate in and out of positions frequently (often less than six months), data are gathered in multiple formats to enter into the system, and the source of the data entering the system is provided by government and non-government organizations that are spread throughout the country. As such, the reliability of the reports generated by IRMS is diminished without assurance that the initial data entering the system are complete, accurate, and valid.

[5] U.S. Government Accountability Office document, *Internal Control Management and Evaluation Tool,* GAO-01-1008G, August 2001.

[6] Army organizations have an alpha/numeric designator which identifies their various command functions, for example, G-2 = Intelligence, G-4 = Logistics, etc. The Communications and Information Technology function is identified by G-6.

Assessment of Computer-Related Controls

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They establish the environment in which application systems and controls operate, and are essential in ensuring data validity, reliability, and accuracy. An effective general control environment would:

- ensure that an adequate computer security management program is in place
- protect data, files, and programs from unauthorized access, modification, disclosure, and destruction
- limit and monitor access to programs and files that control computer hardware and secure applications
- prevent unauthorized programs or unauthorized changes to an existing program from being implemented
- prevent any one individual from controlling key aspects of computer-related operations
- ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption

We used the "Federal Information System Controls Audit Manual," issued by the Government Accountability Office[7] in our assessment of the general controls over IRMS. We identified vulnerabilities and the lack of policies and procedures in the following areas:

- security program planning and management
- access controls
- application software development and change controls
- system software
- segregation of duties
- service continuity

When general controls are weak, they severely diminish the reliability of controls associated with individual applications. As such, there is diminished assurance that there is adequate security and integrity of the data in IRMS that supports program management oversight and decision making.

Security Program Planning and Management

A security management program is the foundation of an organization's security control structure and a reflection of management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for:

- periodically assessing risk
- developing and implementing effective security procedures
- monitoring the effectiveness of these procedures

[7] U.S. Government Accountability Office document, *Federal Information System Controls Audit Manual,* GAO/AIMD-12.19.6, January 1999.

A well-designed security management program helps to ensure that security controls are adequate, properly implemented, and applied consistently across the entity and that responsibilities for security are clearly understood.

Currently there is no approved Security Plan in place for IRMS. However, GRD-PCO G-6 management provided a copy of a draft document entitled, "System Security Authorization Agreement" (SSAA), version 2.0, dated September 6, 2005, which did contain many of the controls prescribed in the Office of Management and Budget (OMB) Circular A-130[8] that could be included in an IRMS security plan. Areas not covered included, application rules, contingency planning, and management authorization of systems to process information.

In addition, numerous draft operating procedures were provided for our review, including those for:

- Managing Electronic Files
- Data Retention and Recovery Policy
- Password Policy
- Remote Access Policy

Further, there are Memorandums of Understanding which were recently signed by the various organizations providing IRRF data to IRMS identifying how the data was to be collected, maintained, and disseminated.

While these individual documents could address some of the requirements of a security program, they were not currently incorporated or referenced in the form of a documented security plan. In addition, there was no formal review/approval by GRD-PCO G-6 management or resource users of the SSAA.

The effective implementation of appropriate, properly designed security controls is an essential element for ensuring the confidentiality, integrity, and availability of information systems and information. Weak security controls can expose information systems and information to an increased risk of unauthorized access, use, disclosure, disruption, modification, and destruction.

Access Controls

Access controls are designed to limit or detect access to computer programs, data, equipment, and facilities to protect these resources from unauthorized modification, disclosure, loss, or impairment. Such controls include logical and physical security controls.

Logical security controls. These measures involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input unique user identifications, passwords, or other identifiers that are linked to predetermined access privileges. Logical security controls restrict the access of legitimate users to the specific systems, programs, and files they need to conduct their work and prevent unauthorized users from gaining access to computer resources.

[8] Appendix III of OMB Circular No. A-130, “Management of Federal Information Resources," established a minimum set of controls for agencies’ automated information security programs, including: application rules, training, personnel controls, incident response capability, contingency planning, technical security, access controls, periodic review of security controls, and management authorization of systems to process information

The GRD-PCO logical security controls restrict access by a series of controls that include passwords and monitoring systems. Passwords are unique for specific individuals, not groups; are controlled by the assigned user and not subject to disclosure; and are changed every 90 days. The monitoring systems ensure redundancy as well as cross verification.

Physical security controls. These methods include door locks, security guards, badges, entry logs, alarms, computer terminal locks, and similar measures (used alone or in combination) that help to safeguard computer facilities and resources from intentional or unintentional loss or impairment by limiting access to the buildings and rooms where they are housed.

Existing GRD-PCO G-6 management operating procedures (Access Control Memorandum and Authorized Access Control List) are posted on the door of the server room. The Access Control Memorandum clearly states that:

> Unescorted access to the network server room will only be granted to members of Office of Information Technology that require routine physical access to equipment in the server room in order to perform their primary job functions and who are on the access list. Exceptions can be made, when warranted, but only by either the Technical Director and/or Operations Deputy. All others will require an escort anytime access is required.

While we did observe that the server room, which houses the servers that all information on the network passes through, is controlled with a cipher lock; our review of physical access controls for IRMS identified the following weaknesses:

- Personnel requiring an escort while in the server room (an expatriate and two local nationals) were left unattended for over twenty minutes.
- There was no record, or visitor’s log, to document personnel not identified on the "Authorized Access Control List" who were granted access to the server room.
- Procedures regarding access controls have not been formalized.

Inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data within IRMS.

Application Software Development and Change Controls

Establishing controls over the modification of application software programs helps to ensure that only authorized programs and authorized modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help to make sure all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs are carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or “turned off,” or that processing irregularities or malicious code could be introduced. Critical elements include:

- Processing features and program modifications are properly authorized
- All new and revised software is tested and approved.
- Software libraries are controlled.

GRD-PCO G-6 management has not established documented policies and procedures for application software development in some key areas. Undocumented and ad hoc practices were identified in both configuration control and test planning.

Processing features and program modifications. GRD-PCO does not have a documented policy and procedure for approving and authorizing configuration changes. However, they have a newly implemented process of submitting changes to a Configuration Control Board (CCB) for review and approval. They also use Tortoise, an automated configuration control software application, to track configuration changes to the application. Establishing the CCB is a positive step to formalizing the control over application development changes; however, without specific policies and procedures governing the role of the CCB and the requirements authorization and approval process, unnecessary or detrimental modifications could be approved.

Testing and approval. GRD-PCO does not have a documented policy or procedure at GRD-PCO G-6 to standardize formal test planning processes. Test planning and execution must be done in methodical, repeatable, and consistent way to ensure the results are credible and complete. At GRD-PCO G-6, approved application requirements are developed into application modifications and tested to the extent deemed necessary by the assigned development team to meet the requirements and to avoid other systems integration interference. The revised capability is demonstrated to the development team, the GRD-PCO G-6 Director of IT, and user representatives to ensure adequacy of the revision. These undocumented and ad hoc testing practices may result in incomplete and unrepeatable results which could allow application errors to go unchecked.

Control software libraries. GRD-PCO IT does not have a policy and procedure which specifically addresses controls for IRMS development files. However, current policies and procedures appear to provide adequate protection for the IRMS database, as well as files created and modified as a part of the IRMS application software, by controlling access, and establishing periodic back-ups. Specifically, the *PCO SOP on IT Access Control & Security (IT-100)*, documents the controls restricting access and level of control for individual or groups of users. Further, the PCO policies on *Data Back-up* and *Data Retention* address the maintenance of the network data files in general.

Copies of software programs should be maintained in carefully controlled libraries. Inadequately controlled software libraries increase the risk that unauthorized changes could be made either inadvertently or deliberately for fraudulent or malicious purposes.

For a more complete description of our assessment of the application software development and change controls, see Appendix B.

System Software

System software includes operating system software; system utilities; program library systems; file maintenance software; security software; data communications systems; and database management systems. System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. Controls over access to and modifications of system software are essential to protect the overall integrity and reliability of information systems.

GRD-PCO G-6 has established adequate policies, procedures, and general controls to limit access to system software, and to monitor unauthorized use or intrusion of system resources. However, GRD-PCO G-6 management has not documented processes for system software control in the area of test planning and execution.

GRD-PCO G-6 does not currently have a documented procedure regarding testing for the system software. Modifications to system software should be controlled so only authorized and properly tested changes are implemented. If system software is not adequately controlled and tested, system parameters may be inadequate to prevent unauthorized changes to application programs or data. Generally, the processes being used by GRD-PCO G-6 support the intent described above, but in an undocumented and ad hoc fashion. Test planning and execution must be done in methodical, repeatable, and consistent way to ensure the results are credible and complete. The use of undocumented and ad hoc testing practices may result in incomplete and unrepeatable results which could allow system errors to go unchecked, jeopardizing the integrity and reliability of the system.

For a more complete description of our assessment of the system software controls, see Appendix B.

Segregation of Duties

Another key control for safeguarding programs and data are to ensure that duties and responsibilities for authorizing, processing, recording, and reviewing data, as well as initiating, modifying, migrating, and testing programs, are separated to reduce the risk that errors or fraud will occur and go undetected. Duties that should be appropriately segregated include applications and system programming and responsibilities for computer operations, security, and quality assurance. Policies outlining the supervision and assignment of responsibilities to groups and related individuals should be documented, communicated, and enforced. Inadequate segregated duties increase the risk that erroneous or fraudulent transactions could be processed, that improper program changes could be implemented, and that computer resources could be damaged or destroyed.

GRD-PCO G-6 has no prescribed policies or operating procedures discussing separation of duties. Employees have documented job descriptions that clearly describe their duties. Management performs a quarterly performance review to ensure assigned responsibilities are accomplished. However, because of the nature of computer operations, these measures do not ensure that personnel only perform authorized activities. As such, policies outlining the responsibilities performed by application programmers, data center staff, and related individuals should be documented, communicated, and enforced. Effective supervision and formal operating procedures are required to help prevent or detect unauthorized or erroneous personnel actions.

Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and post-disaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency. It addresses how an organization will deal with a range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

In reviewing the elements associated with IRMS's service continuity planning, we found that environmental controls associated with the IT hardware within the Server Room appear to be adequate and comply with internal control techniques.

Another critical element of service continuity planning is identifying critical operations and data. The IRMS Project Manager described the recent process the program managers, engineers, and consultants conducted in October and November 2005 to identify and prioritize critical operations and applications. This assessment should provide the IT Director and project managers with reasonable support regarding identifying and prioritizing all critical operations and data in IRMS.

The major risk identified regarding service continuity planning for IRMS is the lack of a contingency plan, which is required by OMB Circular A-130. Potentially the system may not be able to supply critical operations to system users for possibly an extended period of time. A contingency plan for an IT system located in a war zone is not only a requirement, but a critical necessity for continuity of operations.

For a more complete description of our assessment of the service continuity, see Appendix B.

Conclusion and Recommendations

Conclusion

The reliability of the reports generated by IRMS is diminished without assurance that the initial data entering the system are complete, accurate, and valid. Internal control procedures specific to data entry are critical in providing the initial level of confidence that helps ensure completeness, accuracy, and validity of all transactions during processing. It is the basis for establishing the integrity of the data contained in the IT system. In addition, well-designed and properly implemented IT general controls are essential to protect GRD-PCO's computer resources and operational environment from the risks of inappropriate disclosure and modification of sensitive information, misuse or damage of computer resources, and disruption of critical operations.

GRD-PCO has taken many important steps to implement an information security program. Several of the supporting documents plus processes that were not documented appear to be a good start in developing a quality security management program. However, key elements of such a program have not been fully implemented. Weaknesses in information security controls have placed IRMS financial and management information at risk. Implementing an effective information security program could help ensure that known weaknesses affecting the IRMS computing resources are promptly mitigated and that general controls effectively protect its computing environment. Until such improvements are made, there is diminished assurance that there is adequate security and integrity of the data in IRMS that supports program management oversight and decision making.

It is important for IRMO, in coordination with the GRD-PCO and the agencies utilizing IRRF, to continue to provide active leadership in assuring all organizations work together in correcting the problems identified with IRMS.

Recommendations, Management Comments, and Audit Response

We recommend that the Director of the Iraq Reconstruction Management Office develop and issue a policy requiring all organizations entering data into IRMS to have documented internal control procedures that require validation of all data entering the system.

We also recommend that the Commanding General GRD-PCO direct the GRD-PCO G-6 Director of Information Technology to:

- Review all security management program operating procedures to ascertain if they contain current and accurate information and are still applicable to the operation. Those operating procedures which are still valid should then be formally signed and dated by GRD-PCO G-6 Director of IT. Once formalized, the procedures should be distributed and discussed with the IT staff responsible for implementing the procedure, referenced to the IT Security Plan (if applicable), and kept on-site at various locations for reference.

- Document and formalize a security plan for IRMS. The basis for a GRD-PCO IT security plan is contained in the GRD-PCO G-6 draft document, “System Security Authorization Agreement” (SSAA), dated September 6, 2005. A review of the draft SSAA should be conducted to update existing information and to ensure it contains all required elements, as prescribed by OMB Circular A-130, including such topics as application rules and contingency planning. The updated security plan should then be approved by GRD-PCO G-6 Director of IT. Multiple copies of the security plan should be available with some stored at off-site locations.

- Ensure the access control policy posted on the network server room door is adhered to. All unauthorized personnel should be escorted whenever access to the network server room is required, and not left unattended while in the room. In addition, for control purposes, GRD-PCO G-6 should establish a visitor's log to document all personnel escorted into the network server room.

- Develop adequate application software development policies and procedures to establish a formal configuration control process for IRMS. At a minimum, this policy should address the authority of the Configuration Control Board, the requirements authorization and approval process, and the configuration management tracking processes. Policies and procedures should also clearly identify the duties and responsibilities of those identified in the design, development, review, and approval of the system modifications.

- Develop adequate application software development testing policies and procedures to clearly define, at a minimum: the testing methodology to be used; the development of specifications and requirements to be tested; required documentation to be recorded and retained; and levels of testing and associated procedural differences with each level.

- Develop adequate system software control policies and procedures to clearly define, at a minimum: procedures for identifying, selecting, installing, and modifying system software; required documentation to be recorded and retained; and levels of testing and associated procedural differences with each level.

- Develop policies and procedures to clearly delineate separation of duties and responsibilities, including those performed by application programmers, system programmers, and data center, security, and quality assurance staff,

- Develop a contingency plan for restoring critical applications that includes arrangements for alternative processing facilities in case the usual facilities are significantly damaged or cannot be accessed. It is important that these plans be clearly documented, communicated to affected staff, and updated to reflect current operations. Multiple copies of the contingency plan should be available with additional ones stored at off-site locations to make sure they are not destroyed by the same events that made the primary data processing facilities unavailable. In addition, the plan should be tested on an on-going basis to determine whether it will function as intended in an emergency situation. A copy of the contingency plan should be kept in the installation's Security Plan.

Management Comments and Audit Response. A combined response to the draft of this report was received from the U.S. Ambassador of Iraq and IRMO. The U.S. Ambassador to Iraq concurred with the recommendation to develop and issue a policy requiring all organizations entering data into IRMS to have documented internal control procedures that require validation of all data entering the system. The Information Management Unit of IMRO will take the lead. The comments received are fully responsive.

Comments to the draft of this report were also provided by the Commanding General, Gulf Region Division, and have been incorporated into this final report as appropriate. The Commanding General, Gulf Region Division, concurred with all findings in the report and has initiated corrective action on all recommendations. The comments received are fully responsive.

Appendix A. Scope and Methodology

In October 2005, we initiated this audit (Project No. SIGIR-2005-16). Our review was performed at the Freedom Building, the Project and Contracting Office (PCO) Annex, the U.S. Agency for International Development (USAID) Compound, and the U.S. Embassy Annex in the International Zone, Baghdad, Iraq. We interviewed IT personnel from all of the major IRMS user organizations, specifically, the Iraq Reconstruction Management Office (IRMO); U.S. Army Corps of Engineers Gulf Region Division – Project and Contracting Office (GRD-PCO); management officials of the GRD-PCO Communications and Information Technology function (GRD-PCO G-6); the Multi-National Security Transition Command-Iraq; and USAID.

The six major categories of general controls we considered during the review, as identified in the U.S. Government Accountability Office "Federal Information System Controls Audit Manual" were:

- security program planning and management
- access controls
- application software development and change controls
- system software
- segregation of duties
- service continuity

The review did not address controls over individual applications within IRMS.

To assess the information security program for IRMS, we:

- Discussed with IT personnel quality assurance controls over data entry into application systems that subsequently provide data to the IRMS system.

- Reviewed and evaluated IRMS's information security policies and procedures in effect at the time of our review.

- Examined and assessed reports and other documents related to the IRMS information security program.

- Interviewed GRD-PCO G-6 officials regarding their processes and procedures for overseeing, monitoring, evaluating, and reporting on the implementation of information security.

The following criteria were used in determining if the GRD-PCO's IRMS system was in conformance with applicable federal regulations, policies and procedures:

- OMB Circular No. A-130, "Management of Federal Information Resources," November 28, 2000.

- Government Accountability Office publication, "Federal Information System Controls Audit Manual" (FISCAM), GAO/AIMD-12.19.6, January 1999.

- Government Accountability Office publication, "Internal Control and Management Evaluation Tool," GAO-01-1008G, August 2001.

We conducted this audit from October through December 2005, in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not utilize any computer-processed data during this audit.

Prior Coverage.

Special Inspector General for Iraq Reconstruction (SIGIR). Reports issued by the Office of the Special Inspector General for Iraq Reconstruction can be accessed on its website http://www.sigir.mil.

SIGIR Audit Report Number SIGIR-05-027, dated January 27, 2006, "Methodologies for Reporting Cost-to-Complete Estimates", concluded that U.S. government agencies failed to effectively compile and report cost-to-complete information for IRRF projects – Facilities and Transportation (F&T) sector, as required by Public Law 108-106, thereby excluding important project visibility essential for project management and Congress to make informed management decisions during IRRF program execution.

SIGIR Audit Report Number SIGIR-05-021, dated October 24, 2005, "Management of Iraq Relief and Reconstruction Fund Programs: Cost-to-Complete Estimate Reporting", concluded the three organizations responsible for IRRF projects – PCO, USAID, and the Multi-National Security Transition Command-Iraq – have been required, since January 2004, to report cost-to-complete information for their IRRF projects in quarterly reports to the Congress. However, these organizations did not begin providing reasonably comprehensive cost-to-complete data to IRMO until the summer of 2005.

SIGIR Audit Report Number SIGIR-06-001, April 2006, "Management of Iraq Relief and Reconstruction Fund Program: The Evolution of the Iraq Reconstruction Management System", concluded that development of the new unified Iraq Reconstruction Management System (IRMS) showed progress toward meeting the automated support requirements, but there were still problems to resolve relating to data verification before the system would become fully functional.

Department of the Army - U.S. Army Audit Agency. Audit Report Number A-2005-0194-ALA, dated May 26, 2005 "Program Management in Support of Iraq Reconstruction", concluded that while the PCO had established controls for monitoring and measuring obligations, the PCO needed additional controls to account for all DOD activities and to measure the progress of the program.

U.S. Government Accountability Office – Audit Report Number GAO-01-89, dated October 11, 2000, "Financial Management: Significant Weaknesses in Corps of Engineers' Computer Controls."

U.S. Government Accountability Office – Audit Report Number GAO-02-589, dated June 10, 2002, "Information Management: Corps of Engineers Making Improvements, But Weaknesses Continue."

Appendix B. Detailed Assessment of General Controls Using the FISCAM

We used the “Federal Information System Controls Audit Manual (FISCAM),” issued by the Government Accountability Office[9] in our assessment of the general controls over IRMS.

General controls are the structure, policies, and procedures that apply to an entity’s overall computer operations. They establish the environment in which application systems and controls operate. General controls include a security management program, access controls, system software controls, application software development and change controls, segregation of duties, and service continuity controls. An effective general control environment would (1) ensure that an adequate computer security management program is in place, (2) protect data, files, and programs from unauthorized access, modification, disclosure, and destruction, (3) limit and monitor access to programs and files that control computer hardware and secure applications, (4) prevent unauthorized programs or unauthorized changes to an existing program from being implemented, (5) prevent any one individual from controlling key aspects of computer-related operations, and (6) ensure the recovery of computer processing operations in case of a disaster or other unexpected interruption.

This appendix provides details on our assessment regarding:

- Application software development and change controls
- System software controls
- Service continuity

Application Software Development and Change Controls

Controls over the modification of application software programs help to ensure that only authorized programs and authorized modifications are implemented. These controls help ensure that all programs and program modifications are properly authorized, tested, and approved and that access to and distribution of programs is carefully controlled. Without proper controls, there is a risk that security features could be inadvertently or deliberately omitted or “turned off” or that processing irregularities or malicious code could be introduced.

Processing features and program modifications. The processing features built into application software should be authorized by the managers responsible for the agency program or operations that the application supports. The IRMS Information Technology Working Group performs this critical function by developing, defining, and approving the baseline requirements and the Configuration Control Board (CCB) act to approve required revisions from the baseline. The GRD-PCO IT management group then implements, maintains, and controls the configuration of the applications software.

The Application Development Lead indicated that a formal Software Development Life Cycle (SDLC) methodology was not being used in support of IRMS. In relatively uncomplicated software developments where the design is primarily an integration and adaptation of previously developed (commercial item or Government item) software, implementation of a formal SDLC program is not generally required. However, it appears

[9] U.S. Government Accountability Office document, *Federal Information System Controls Audit Manual,* GAO/AIMD-12.19.6, January 1999.

that the major tenants of an SDLC program were being accomplished in the form of a structured approach with active user involvement through on-going communication within the IRMS Information Technology Working Group training sessions, and Maximo user group meetings. User training is provided focusing on basic, advanced, and customized levels of instruction. A formalized configuration control process is utilized (discussed below). Detailed specifications relative to each principle user group are developed from a common specifications template. This template uses a common data dictionary to map specific organizational data into the IRMS system to ensure data integrity and completeness in the transfer.

GRD-PCO IT has not documented its policy and procedure for approving and authorizing configuration changes; however, they have a newly implemented process of submitting changes to a CCB for review and approval. They also use Tortoise, an automated configuration control software application, to track configuration changes to the application. We believe that establishing the CCB is a positive step to formalizing the control over application development changes. However, without specific documented policies and procedures governing the role of the CCB and the requirements authorization and approval process, unnecessary or detrimental modifications could be approved.

It is important that an entity have clear policies regarding the use of personal and public domain software by employees at work. Allowing employees to use their own software or external data storage devices that have been used elsewhere, increases the risk of introducing viruses. It also increases the risk of violating copyright laws.

We found that policies and procedures are in place by the GRD-PCO Information Assurance (IA) office to ensure that only approved software is installed on the system computers. This is a critical control point to reduce the likelihood of the introduction of a virus or copyright law violations. The IA Office must approve any exceptions to the approved list of software installed on system computers.

Testing and approval. A disciplined process for testing and approving new and modified programs prior to their implementation is essential to make sure programs operate as intended and that no unauthorized changes are introduced. The extent of testing varies depending on the type of modification. For new systems being developed or major system enhancements, testing will be extensive, generally progressing through a series of test stages that include (1) testing individual program modules (unit testing), (2) testing groups of modules that must work together (integration testing), and (3) testing an entire system (system testing). Minor modifications may require less extensive testing; however, changes should still be carefully controlled and approved since relatively minor program code changes, if done incorrectly, can have a significant impact on overall data reliability. During our interviews with the Application Development Lead we were told that the application changes were primarily modifications of commercially available software packages and the integration of these packages. This official believed that this relatively simple application development approach did not warrant the same level of testing rigor that a bottom-up design and development software program would require.

GRD-PCO has not documented its policy or procedure to standardize formal test planning processes. Test planning and execution must be done in methodical, repeatable, and consistent way to ensure the results are credible and complete. At GRD-PCO IT, approved application requirements are developed into application modifications and tested to the extent deemed necessary by the assigned development team to meet the requirements and to avoid other systems integration interference. The revised capability is demonstrated to the development team, the Director of IT, and user representatives to ensure adequacy of the revision. However, these undocumented and ad hoc testing practices may result in incomplete and unrepeatable results which could allow application errors to go unchecked.

Control software libraries. To ensure that approved software programs are protected from unauthorized changes or impairment and different versions are not misidentified, copies should be maintained in carefully controlled libraries. Further, adequately controlled software libraries help ensure that there is (1) a copy of the “official” approved version of a program available in case the integrity of an installed version is called into question and (2) a permanent historical record of old program versions.

The *PCO SOP on IT Access Control & Security (IT-100),* documents the controls restricting access and level of control for individual or groups of users. Further, the PCO policies on *Data Back-up* and *Data Retention* address the maintenance of the network data files in general. We found that current policies and procedures appear to provide adequate protection for the IRMS database by controlling access, and establishing periodic back-ups. Additionally, files created and modified as part of the IRMS application software may also be adequately protected under the above policies and procedures. However, GRD-PCO IT does not have a policy and procedure which specifically addresses IRMS development files.

Further, testing policy and procedures are not formally established. The FISCAM indicates several formal documentation requirements to define testing procedures and the track the execution of the testing. These procedures are necessary in any development effort. Regardless of project scope, policies and procedures should be properly established and test plans should be properly documented.

System Software Controls

System software coordinates and helps control the input, processing, output, and data storage associated with all of the applications that run on a system. System software includes operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems. Controls over access to and modifications of system software are essential to protect the overall integrity and reliability of information systems.

During our interviews, the GRD-PCO G-6 Information Assurance Manager described the policies and procedures utilized to support the system software administration of the network supporting IRMS. Based on our review of the policies and procedures, we determined that it appears that GRD-PCO G-6 has established adequate policies, procedures, and general controls to limit access to system software and to monitor unauthorized use or intrusion of system resources. However, GRD-PCO G-6 management had not documented its policies and procedures for system software control in the area of test planning and execution.

Limit access to system software. Access to system software should be restricted to a very limited number of personnel whose job responsibilities require they have such access. GRD-PCO G-6 limits access to the system software to the people assigned to the systems administration section under the GRD-PCO G-6 Director of IT. Further, domain system administrative permissions are limited to only five of these system administrators. GRD-PCO G-6 uses the practice of *least privilege* to restrict a user’s access to the *minimum* necessary to perform the job.

In order to control access, it is essential to analyze the system software configuration to identify all paths through which access to sensitive capabilities can be obtained. The *PCO Network & Systems Operations Manual* identifies a variety of functions required to be performed periodically by the IA team to mitigate risk on the PCO-IRAQ.NET network. These requirements in part include: assessing signature files; anti-virus scans; malicious code identification; and vulnerability assessments. Additionally, a LINUX based SNORT application is used as an intrusion detection system. The SNORT intrusion detection system was recently installed to provide an active monitoring capability.

<u>Monitor access to and use of system software</u>. Because of the powerful capabilities at the disposal of those who have access to system software, its use should be monitored to identify any inappropriate or unusual behavior. GRD-PCO G-6 uses a combination of monitoring practices and software utilities. In addition to the intrusion detection system, the Kiwi Syslog Daemon is used to monitor server logs. There are also three redundant network primary monitoring systems employed: Cisco Works 2000, SolarWinds Network Performance Monitor, and the Crannog Netflow Monitor. These systems provide overlapping coverage in monitoring the systems and provides for cross verification. The use of these monitoring procedures is discussed in the *PCO Network & Systems Operations Manual*.

When questionable activity is identified, it should be investigated. If improper activity is determined to have occurred, in accordance with security violation policies, the incident(s) should be documented, appropriate disciplinary action should be taken, and higher level management notified. The IA manager indicated that GRD-PCO G-6 conducts a routine monitoring of the system as previously described. Any unusual activity is identified, tracked, and further investigated until the incident is resolved.

<u>Control system software changes.</u> Modifications to system software should be controlled so that only authorized and properly tested changes are implemented. If system software is not adequately controlled and tested, system parameters may be inadequate to prevent unauthorized changes to application programs or data. An organization should have a standard procedure for identifying, selecting, installing, and modifying system software to meet its operational needs. System software changes may be needed to correct identified problems, to install a vendor's latest system software version, or to enhance operational efficiencies. All changes should be made under a controlled environment to protect system software integrity. Procedures should exist to identify and document system software problems along with their related analysis and resolution. Specifically, system software problems should be recorded in a log that identifies the problem, the individual assigned to analyze the problem, and how the problem was resolved. All changes should be supported with a request for change document that includes a stated purpose for the change and an authorization to make the change. Error and change documentation and recording is essential in preserving the history of system modifications. This will assist with assessing long-term systemic problems that may be recurring and with establishing a means to pass down information useful in follow-on diagnostics. Preservation of system knowledge is also critical during personnel absences and turnover.

GRD-PCO G-6 does not currently have a documented policy and procedure regarding testing for the system software. Modifications to system software should be controlled so that only authorized and properly tested changes are implemented. If system software is not adequately controlled and tested, system parameters may be inadequate to prevent unauthorized changes to application programs or data. Generally, the processes being used by GRD-PCO G-6 support the intent described above, but in an undocumented and ad hoc fashion. Test planning and execution must be done in methodical, repeatable, and consistent way to ensure the results are credible and complete. The use of undocumented and ad hoc testing practices may result in incomplete and unrepeatable results which could allow system errors to go unchecked, jeopardizing the integrity and reliability of the system.

Testing is conducted in a controlled environment utilizing servers mounted on the "Test Rack" prior to installation on the "Back Office" or production servers. According to the IA manager major changes are approved and documented in detail similar to those in the *IT Manual – Designing & Implementation Plan for PCO Computer Network: Volume I*. and the *Active Directory Setup and Exchange Migration Plan* examples provided for review.

GRD-PCO G-6 reviews the optional features and determines which to enable and disable. Baseline security feature settings are documented in the GRD-PCO G-6: *IT Manual – Designing & Implementation Plan for PCO Computer Network: Volume I*.

GRD-PCO G-6 generally will maintain the previous versions of system software in an isolated server until the replacement software is deemed to be working correctly. Typically 30 days is adequate to effect the transition. All licenses and documentation is current and up-to-date. They are maintained online for easy reference. The online documentation was reviewed and appeared current. GRD-PCO IT also uses the Windows Server Update Services, an automated patch management tool to keep workstations up-to-date with the latest Microsoft patches and hotfixes. Windows Server Update Services plays a big role in protecting workstations from malicious code and viruses. Other software vulnerabilities are determined by conducting weekly scans and vulnerability assessments on the network.

GRD-PCO G-6 has a process to conduct software testing in a controlled environment. They do not currently have a documented policy or procedure for identifying, selecting, installing, and modifying system software to meet its operational needs. Additionally, they do not have a process, policy, or procedure in place to capture and record non-routine system error events; however, there is a process in place for the helpdesk technicians to track IRMS daily activities and trouble tickets using the Maximo program.

Service Continuity

An organization's ability to accomplish its mission can be significantly affected if it loses the ability to process, retrieve, and protect information that is maintained electronically. For this reason, organizations should have (1) established procedures for protecting information resources and minimizing the risk of unplanned interruptions and (2) plans for recovering critical operations should interruptions occur. A contingency or disaster recovery plan specifies emergency response, backup operations, and post-disaster recovery procedures to ensure the availability of critical resources and facilitate the continuity of operations in an emergency. It addresses how an organization will deal with a range of contingencies, from electrical power failures to catastrophic events, such as earthquakes, floods, and fires. The plan also identifies essential business functions and ranks resources in order of criticality. To be most effective, a contingency plan should be periodically tested in disaster simulation exercises and employees should be trained in and familiar with its use.

In reviewing the elements associated with IRMS's service continuity planning, we found that environmental controls associated with the IT hardware within the Server Room appear to be adequate and comply with associated internal control techniques. The server room power supply came from the building's power grid (city power). In case of power failure, a 40 kilovolt ampere (KVA) generator is located on the ground floor of the building and can provide up to one and a half hours of uninterrupted power supply to the server room allowing the servers to be brought down slowly in order not to lose data. The UPS is tested once a week to assure its operational capability. In addition, the UPS is networked to the system for monitoring purposes and all anomalies are reported to the network. There were no plumbing or water lines in the room.

The following environmental controls were identified in the server room:

- Four CO_2 fire extinguisher canisters – one located at the entrance to the room and the other three at various locations in the room.
- One main air conditioner unit and four smaller units providing redundancy – preventive maintenance on the air conditioner units is done monthly.
- One fan for air circulation.

Another critical element of service continuity planning is identifying critical operations and data. The IRMS Project Manager described the recent process the program managers, engineers, and consultants went through in October and November 2005 to identify and prioritize critical operations and applications. The process assigned all applications in the IRMS core a numeric score (1-3) as to the criticality of the application. In addition, all system software was documented on a data sheet identifying items such as: criticality (numeric score 1-5), primary function, technical point-of-contact, administrative point-of-contact, resident server, services provided, and a diagram showing which other systems the system receives input from and sends output to. The above assessment provides the IT Director and project managers with reasonable support regarding identifying and prioritizing all critical operations and data in IRMS.

The major risk we identified regarding service continuity planning for IRMS is the lack of a contingency plan. The lack of a contingency plan, in addition to being in non-compliance with OMB Circular A-130, leads to the system not being able to supply critical operations to system users for possibly extended periods of time. A contingency plan for an IT system located in a war zone is not only a requirement but a critical necessity for continuity of operations.

Appendix C. Acronyms

CCB	Configuration Control Board
FISCAM	Federal Information System Controls Audit Manual
GRD	Gulf Region Division
GRD-PCO	Gulf Region Division - Project and Contracting Office
IA	Information Assurance
IRMO	Iraq Reconstruction Management Office
IRMS	Iraq Reconstruction Management System
IRRF	Iraq Relief and Reconstruction Fund
IT	Information Technology
OMB	Office of Management and Budget
PCO	Project and Contracting Office
SDLC	Software Development Life Cycle
SIGIR	Special Inspector General for Iraq Reconstruction
SSAA	System Security Authorization Agreement
USAID	U.S. Agency for International Development

Appendix D. Report Distribution

Department of State

Secretary of State
    Senior Advisor to the Secretary and Coordinator for Iraq
U.S. Ambassador to Iraq
    Director, Iraq Reconstruction Management Office
    Mission Director-Iraq, U.S. Agency for International Development
Inspector General, Department of State

Department of Defense

Secretary of Defense
Deputy Secretary of Defense
    Director, Defense Reconstruction Support Office
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Inspector General, Department of Defense
Director, Defense Contract Audit Agency
Director, Defense Finance and Accounting Service
Director, Defense Contract Management Agency

Department of the Army

Assistant Secretary of the Army for Acquisition, Logistics, and Technology
    Principal Deputy to the Assistant Secretary of the Army for Acquisition, Logistics, and Technology
    Deputy Assistant Secretary of the Army (Policy and Procurement)
    Director, Project and Contracting Office
    Commanding General, Joint Contracting Command-Iraq/Afghanistan
Assistant Secretary of the Army for Financial Management and Comptroller
Chief of Engineers and Commander, U.S. Army Corps of Engineers
    Commanding General, Gulf Region Division
Auditor General of the Army

U.S. Central Command

Commanding General, Multi-National Force-Iraq
    Commanding General, Multi-National Security Transition Command-Iraq
    Commander, Joint Area Support Group-Central

Other Federal Government Organizations

Director, Office of Management and Budget
Comptroller General of the United States
Inspector General, Department of the Treasury
Inspector General, Department of Commerce
Inspector General, Department of Health and Human Services
Inspector General, U.S. Agency for International Development
President, Overseas Private Investment Corporation
President, U.S. Institute for Peace

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

U.S. Senate

Senate Committee on Appropriations
  Subcommittee on Defense
  Subcommittee on State, Foreign Operations and Related Programs
Senate Committee on Armed Services
Senate Committee on Foreign Relations
  Subcommittee on International Operations and Terrorism
  Subcommittee on Near Eastern and South Asian Affairs
Senate Committee on Homeland Security and Governmental Affairs
  Subcommittee on Federal Financial Management, Government Information and International Security
  Subcommittee on Oversight of Government Management, the Federal Workforce, and the District of Columbia

U.S. House of Representatives

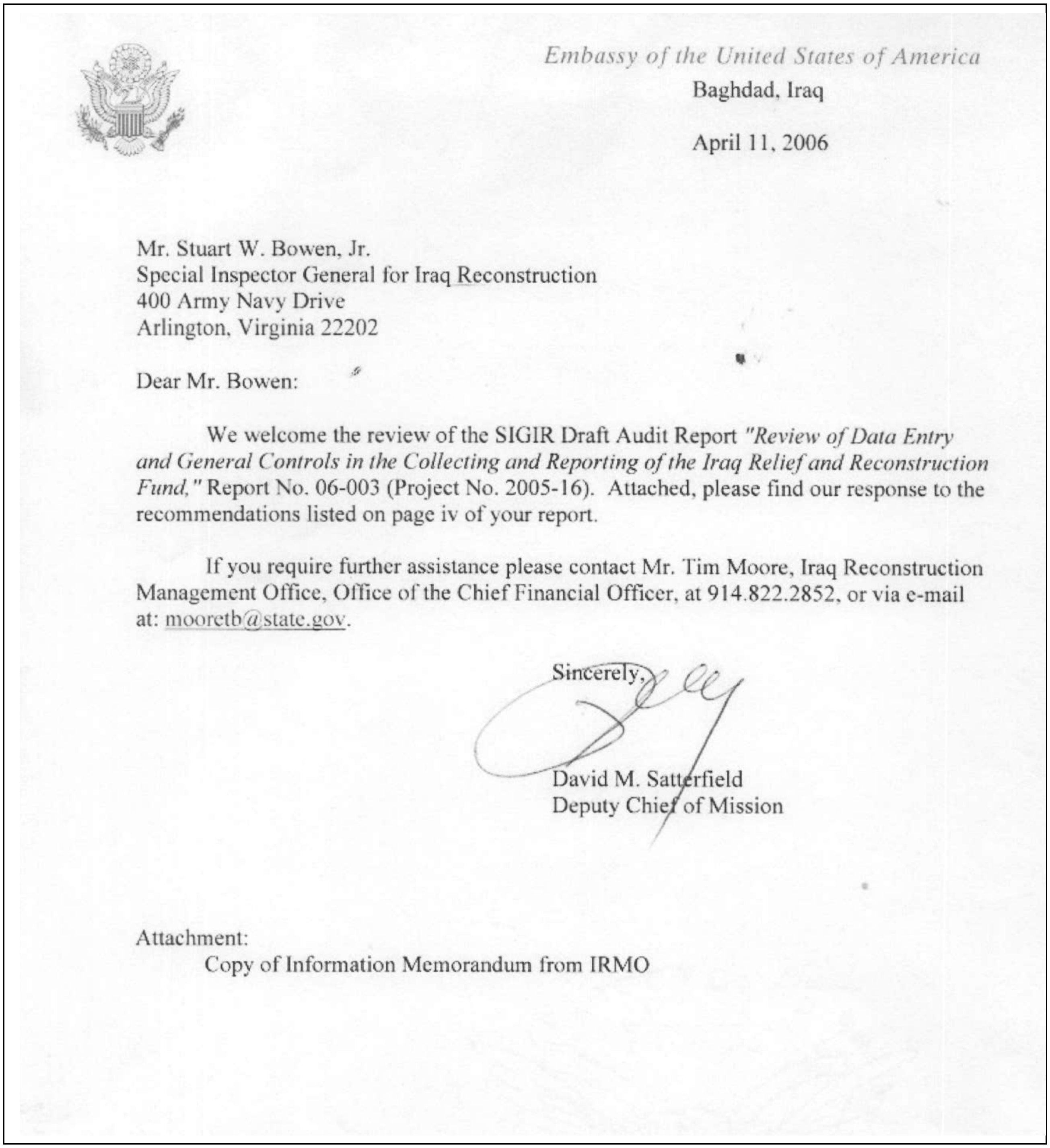
House Committee on Appropriations
  Subcommittee on Defense
  Subcommittee on Foreign Operations, Export Financing and Related Programs
  Subcommittee on Science, State, Justice and Commerce and Related Agencies
House Committee on Armed Services
House Committee on Government Reform
  Subcommittee on Management, Finance and Accountability
  Subcommittee on National Security, Emerging Threats and International Relations
House Committee on International Relations
  Subcommittee on Middle East and Central Asia

Appendix E. Audit Team Members

This report was prepared and the audit was conducted under the direction of Joseph T. McDermott, Assistant Inspector General for Audit, Office of the Special Inspector General for Iraq Reconstruction. The staff members who contributed to the report include:

W. Dan Haigler
Walt Keays
Ronald Rembold

Management Comments
U.S. Ambassador to Iraq



Embassy of the United States of America
Baghdad, Iraq

April 11, 2006

Mr. Stuart W. Bowen, Jr.
Special Inspector General for Iraq Reconstruction
400 Army Navy Drive
Arlington, Virginia 22202

Dear Mr. Bowen:

We welcome the review of the SIGIR Draft Audit Report *"Review of Data Entry and General Controls in the Collecting and Reporting of the Iraq Relief and Reconstruction Fund,"* Report No. 06-003 (Project No. 2005-16). Attached, please find our response to the recommendations listed on page iv of your report.

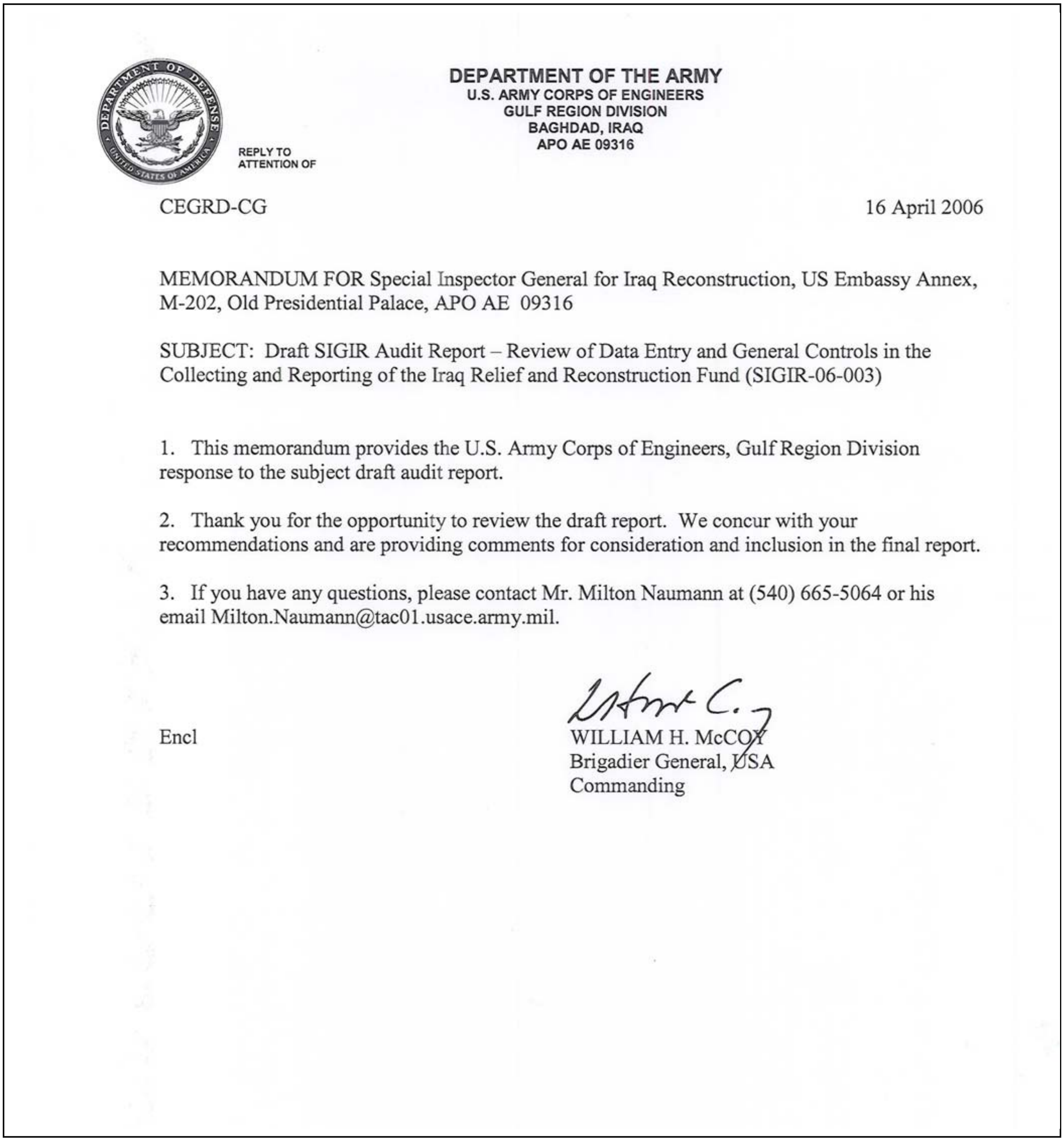
If you require further assistance please contact Mr. Tim Moore, Iraq Reconstruction Management Office, Office of the Chief Financial Officer, at 914.822.2852, or via e-mail at: mooretb@state.gov.

Sincerely,

David M. Satterfield
Deputy Chief of Mission

Attachment:
Copy of Information Memorandum from IRMO

Management Comments
Commanding General, Gulf Region Division,
U.S. Army Corps of Engineers



DEPARTMENT OF THE ARMY
U.S. ARMY CORPS OF ENGINEERS
GULF REGION DIVISION
BAGHDAD, IRAQ
APO AE 09316

REPLY TO
ATTENTION OF

CEGRD-CG

16 April 2006

MEMORANDUM FOR Special Inspector General for Iraq Reconstruction, US Embassy Annex, M-202, Old Presidential Palace, APO AE 09316

SUBJECT: Draft SIGIR Audit Report – Review of Data Entry and General Controls in the Collecting and Reporting of the Iraq Relief and Reconstruction Fund (SIGIR-06-003)

1. This memorandum provides the U.S. Army Corps of Engineers, Gulf Region Division response to the subject draft audit report.

2. Thank you for the opportunity to review the draft report. We concur with your recommendations and are providing comments for consideration and inclusion in the final report.

3. If you have any questions, please contact Mr. Milton Naumann at (540) 665-5064 or his email Milton.Naumann@tac01.usace.army.mil.

Encl

WILLIAM H. McCOY
Brigadier General, USA
Commanding